

**THE CLAIMS:**

Please cancel claim:

constitute the following new

Please do not  
constitute the fo

1           --14. A method for verifying a signature, or respectively an  
 2 authentication, utilizing an asymmetric private-key and public-key cryptographic  
 3 calculation process between a "prover" entity and a "verifier" entity, wherein the  
 4 prover entity performs first cryptographic calculations with said private key to  
 5 produce a signature calculation, or respectively an authentication value  
 6 constituting a response value, and the verifier entity, based on said response  
 7 value, performs second cryptographic calculations with said public key to  
 8 perform said signature verification, or respectively said authentication, the first  
 9 and second cryptographic calculations serving to implement the calculation of  
 10 modulo-n or large-number multiplications, characterized in that for a  
 11 cryptographic calculation process using a public key comprising a public  
 12 exponent e and a public modulo n, and a private key comprising a private  
 13 exponent, it comprises the following steps"

- 14           - calculating at the level of said prover entity at least one prevalidation  
 15 value;
- 16           - transmitting from the prover entity to the verifier entity at least said one  
 17 prevalidation value, and utilizing said prevalidation value by the verifier entity to  
 18 perform at least one modular reduction without any division operation for said  
 19 modular reduction.

1           15. A method according to claim 14, characterized in that for a public  
 2 exponent  $e=2$ , and wherein the cryptographic calculation process is based on a  
 3 RABIN algorithm, said at least one prevalidation value comprises a unique value,  
 4 which is the quotient Q of the square of said respective value of a signature or a  
 5 response by said public modulo n,  $Q = R^2/n$ , where R designates said  
 6 respective value of a signature or a response to an authentication.

1           16. A method according to claim 15, characterized in that after the  
 2 reception by said entity of said respective value of a response to an  
 3 authentication verification or a signature of a message (M), and of said at least

one prevalidation value comprising said quotient, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference ( $D_{AR}$ ,  $D_{SR}$ ) between the square of the response value  $R^2$  and the product  $Q \cdot n$  of said quotient  $Q$  by said public modulo  $n$ , ( $D_{AR}$ ,  $D_{SR} = R^2 - Q \cdot n$ ); and

- verifying the equality of said difference with the value of a function of said response value, without any division operation by the modulo  $n$  operation.

17. A method according to claim 14, characterized in that for a public exponent  $e = 3$ , and wherein the cryptographic calculation process is based on an RSA algorithm, said at least one prevalidation value comprises:

- a first quotient  $Q_1$  of the square  $R^2$  of said response value  $R$  by said public modulo  $n$ ; and

- a second quotient  $Q_2$  of the product of said response value and the difference between the square  $R^2$  of said response value and the product of said first quotient  $Q_1$  and the public modulo  $n$ , by said public modulo  $n$ ,  $Q_2 = R \cdot (R^2 - Q_1 \cdot n) / n$ .

18. A method according to claim 17, characterized in that after the reception of said response value  $R$  and said at least one prevalidation value comprising said first and second quotients  $Q_1$  and  $Q_2$ , said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference ( $D_{ARSA}$ ,  $D_{SRSA}$ ) between the product of said response value  $R$  and the difference between the square  $R^2$  of this response value and the product of said first quotient  $Q_1$  and the public modulo  $n$ , and the product of said second quotient  $Q_2$  and said public modulo  $n$  ( $D_{ARSA}$ ,  $D_{SRSA} = R \cdot (R^2 - Q_1 \cdot n) - Q_2 \cdot n$ ); and

- verifying the equality of this difference with the value of a function of said response value, without any division operation by modulo  $n$  operation.

1 19. A method according to claim 16, characterized in that for an  
2 operation for verifying a signature of a message (M), said function comprising a  
3 standardized public function  $f(M)$  of said message M, said method comprises the  
4 following steps:  
5 - applying a condensation function to said message to obtain a message  
6 digest CM; and  
7 - concatenating said message digest with a constant value.

1 20. A method according to claim 18, characterized in that for an  
2 operation for verifying a signature of a message (M), said function comprising a  
3 standardized public function  $f(M)$  of said message M, said method comprises the  
4 following steps:  
5 - applying a condensation function to said message to obtain a message  
6 digest CM; and  
7 - concatenating said message digest with a constant value.

1 21. A method according to claim 16, characterized in that, for an  
2 authentication verification operation, said method further comprises the step for  
3 transmitting a prompt value from the verifier entity to the prover entity.

1 22. A method according to claim 18, characterized in that, for an  
2 authentication verification operation, said method further comprises the step for  
3 transmitting a prompt value from the verifier entity to the prover entity.

1 23. A method according to claim 21, characterized in that said prompt  
2 value comprises a random value A modulo n, said response value R comprises  
3 an encrypted value B, and said function of the response value comprises a  
4 function  $f(A)$  of said random value A.

1           24. A method according to claim 22, characterized in that said prompt  
2 value comprises a random value A modulo n, said response value R comprises  
3 an encrypted value B, and said function of the response value comprises a  
4 function  $f(A)$  of said random value A.

1           25. A method according to claim 16, characterized in that said function  
2  $f(A)$  of said random value A comprises a function among the functions  $f(A) = A$ ,  
3  $f(A) = n-A$ ,  $f(A) = C \cdot A$  modulo n,  $f(A) = -C \cdot A$  modulo n.

1           26. A method according to claim 21, characterized in that said function  
2  $f(A)$  of said random value A comprises a function among the functions  $f(A) = A$ ,  
3  $f(A) = n-A$ ,  $f(A) = C \cdot A$  modulo n,  $f(A) = -C \cdot A$  modulo n.

1           27. A method according to claim 22, characterized in that said function  
2  $f(A)$  of said random value A comprises a function among the functions  $f(A) = A$ ,  
3  $f(A) = n-A$ ,  $f(A) = C \cdot A$  modulo n,  $f(A) = -C \cdot A$  modulo n.

1           28. A method according to claim 25, characterized in that at the level of  
2 the verifier entity, the calculation of said function  $f(A) = C \cdot A$  modulo n comprises  
3 calculation of the value  $C \cdot A$  and storing of said value if  $C \cdot A < n$ , and the  
4 calculation and storing of the value  $C \cdot A - n$  if not, and in that calculation of said  
5 function  $f(A) = -C \cdot A$  modulo n comprises calculation of the value  $n - C \cdot A$  and  
6 storing of said value if  $n - C \cdot A \geq 0$ , and otherwise calculation of the intermediate  
7 value  $C \cdot n - C \cdot A$ , and if said intermediate value is greater than or equal to zero,  
8 calculation and storing of the value of  $-C \cdot A$  modulo n, for verifying the equality of  
9 said authentication without any division for the modular reduction.

1           29. A method according to claim 26, characterized in that at the level of  
2 the verifier entity, the calculation of said function  $f(A) = C \cdot A$  modulo n comprises  
3 calculation of the value  $C \cdot A$  and storing of said value if  $C \cdot A < n$ , and the

4 calculation and storing of the value  $C \cdot A - n$  if not, and in that calculation of said  
 5 function  $f(A) = -C \cdot A \text{ modulo } n$  comprises calculation of the value  $n - C \cdot A$  and  
 6 storing of said value if  $n - C \cdot A \geq 0$ , and otherwise calculation of the intermediate  
 7 value  $C \cdot n - C \cdot A$ , and if said intermediate value is greater than or equal to zero,  
 8 calculation and storing of the value of  $-C \cdot A \text{ modulo } n$ , for verifying the equality of  
 9 said authentication without any division for the modular reduction.

1 30. A method according to claim 27, characterized in that at the level of  
 2 the verifier entity, the calculation of said function  $f(A) = C \cdot A \text{ modulo } n$  comprises  
 3 calculation of the value  $C \cdot A$  and storing of said value if  $C \cdot A < n$ , and the  
 4 calculation and storing of the value  $C \cdot A - n$  if not, and in that calculation of said  
 5 function  $f(A) = -C \cdot A \text{ modulo } n$  comprises calculation of the value  $n - C \cdot A$  and  
 6 storing of said value if  $n - C \cdot A \geq 0$ , and otherwise calculation of the intermediate  
 7 value  $C \cdot n - C \cdot A$ , and if said intermediate value is greater than or equal to zero,  
 8 calculation and storing of the value of  $-C \cdot A \text{ modulo } n$ , for verifying the equality of  
 9 said authentication without any division for the modular reduction.

1 31. A method according to claim 23, characterized in that said function  
 2  $f(A)$  of said random value  $A$  is the function  $f(A) = A$ , which makes it possible to  
 3 verify the equality of said difference and the validity of said authentication without  
 4 any division operation for the modular reduction.

1 32. A method according to claim 24, characterized in that said function  
 2  $f(A)$  of said random value  $A$  is the function  $f(A) = A$ , which makes it possible to  
 3 verify the equality of said difference and the validity of said authentication without  
 4 any division operation for the modular reduction.

1 33. A method according to claim 14, characterized in that said  
 2 response value, an encrypted value  $B$ , and a quotient value  $Q$  are concatenated  
 3 prior to transmission of the values from the prover entity to the verifier entity.

$$a^6$$
2  
3

9